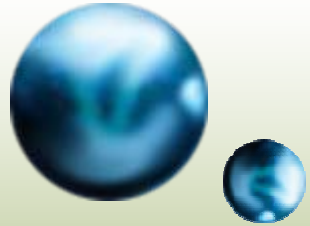
Service Oriented Architecture and Identity Management & Authentication

California Enterprise Architecture Program

March 29, 2006

Introduction

California Enterprise Architecture



- What is CEAP?
- Why SOA / Identity
- Relation to the IT Strategic Plan

SOA

What is SOA

- Open, web-based architecture
- Platform & language independent
- XML message based
- Highly interoperable
- Location transparency
- Many security features
- Wide vendor support
- Direct support for business services
- More than Web Services
  - SOA provides the application and integration infrastructure for a web services-based environment

California SOA Goals

- Provide the blueprint for a service oriented architecture that supports California business services and incorporates Identity concepts.
- Provide a key set of SOA principles.
- Ensure SOA fits into the California Enterprise Architecture model.
- Establish a California SOA Center of Excellence to provide SOA leadership, governance, and management of SOA components.

California SOA Principles

1. Design for ease of use
2. Design web services with appropriate granularity
3. Reassemble before Rewrite
4. Design loosely coupled web services
5. Web services must have well defined interfaces
6. Design stateless base web services

   (doesn't require knowledge of actions taken by a different web service)

California SOA Principles

7. Implement business processes via orchestrating web services
8. Governance & funding structures must be created to manage web service development, deployment and operational environments
9. Implement web services security and policy enforcement standards
10. Provide for transaction failures

    (design services so all transaction items either succeed or rollback)

BRM and SRM Example

	Business Reference Model				Service Reference Model			
Customer Audience	**Business Service Group**	**Line Of Business**	**Business Function**	**Business Service**	**Service Domains**	**Service Types**	**Service Components**	**WS Type**
C2G	Regulatory & Compliance	Licensing	Professional Licensing	Medical Doctor License	Business Management Services	Payment Services	Credit Card Payment Service	Base
						Customer Services	Address Verification Service	Base
					Authorization Services	Professional License Qualifying Services	Check Criminal Background Service	Base
							Check License Qualifications Service	Base
							Check Qualifications Fulfillment Service	Base
C2G	Financial Assistance	Title IV Grants	Post-Secondary Education	Cal-Grant	Business Management Services	Payment Services	EFT Payment Service	Base
					Grants Service	Grant Eligibility Services	Student Financial Eligibility Service	Base
							Student Academic Eligibility Service	Base
B2G	Revenue Collection	Business Tax Payments	Employer Income Taxes	Personal Income Tax	Business Management	Payment Services	Business Payment Service	Composite
				State Disability Tax	Reporting Services	Employer Reporting Services	Base Wage Reporting Service	Base
B2G	Regulatory & Compliance	Licensing	Permits	Encroachment Permit	Business Management Services	Payment Services	EFT Payment Service	Base
							Credit Card Payment Service	Base
					Electronic Delivery Services	Issuance Services	Issue Permit Service	Base
						Confirmation Services	Email Confirmation Service	Base
E2G	Government Services Management	HR Management	Organization & Position	Position Control	Employee Services	Position Tracking	Personnel Transaction	Base
				Employee History		Emp Pos Track		
			Compensation Management	Salary & Leave		Comp Tracking		
				Time & Attendence		Attend Tracking		

Governance

Enterprise Issues

- How will shared services be governed?
- How will shared services be funded?
- How will shared service components be mapped to business services?
- How will component versioning and release packaging be controlled?
- How will components be certified?
- How will component usage be inventoried and tracked?
- How will enterprise troubleshooting be handled?
- How will developers be supported?

Enterprise Issues

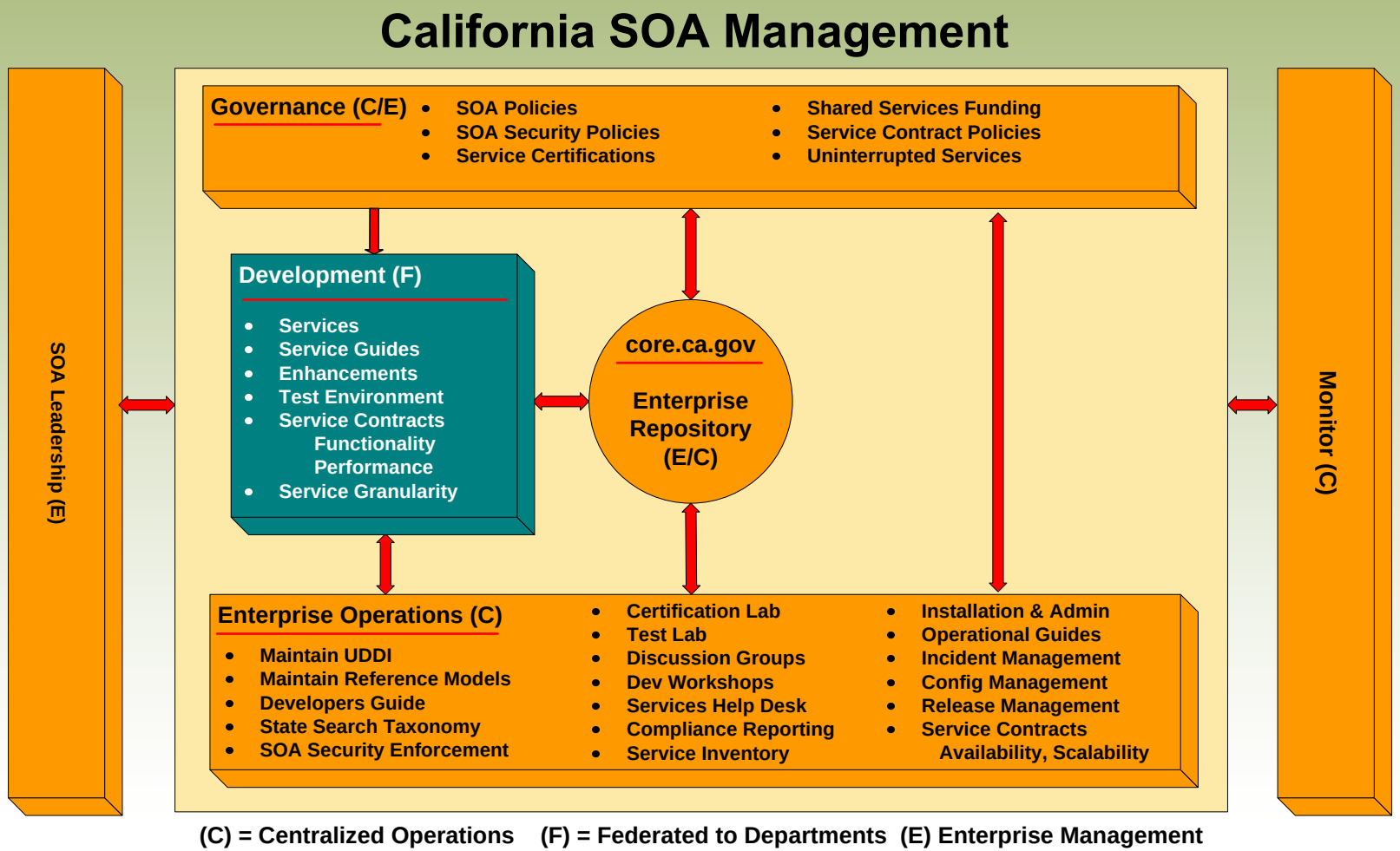
- How will components be tested for performance, availability, scalability?
- How will developers locate code for an existing service?
- How will enterprise components be promoted and marketed?
- Will there be a centralized SOA help desk?
- How will business and technical architects determine which components already exist?
- Will there be demo applications?
- Will there be a state-wide search service using a common language?

SOA Excellence Model

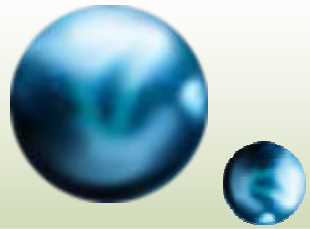
Centralized vs Federated

- A successful state-wide SOA program will require both centralized and federated components
- Singular vision & goals, governance, enterprise repository management, and many operational functions should be **centralized**
- Service development should be **federated** to the producing departments.

Centralized Operations Model



Why is Governance Important



- Minimizes “service chaos”
- Provides uniform service development and deployment
- Enforces standards
- Enforces consistent security policies
- Reduces overall IT cost
- Provides inventory of services
- Resolves shared services and enterprise services funding issues

Architecture

Web Services

- A service in SOA is an application function packaged as a **reusable** component for use in a business process.
- Web Services stress **interoperability** and **location transparency**. (XML/HTTP/SOAP/WSDL/UDDI)
- Web Services are **language agnostic** and **platform independent**. (XML interfaces)
- Web Services use web based messaging:
  - SOAP/HTTP (WSDL)
  - HTTP-GET (REST)
  - HTTP-POST
- Web Services directly support Business Services
  - Service Reference Model & Business Reference Model

Web Service Types

- Base Web Service (fine-grained)
  - Stateless, encapsulated information
  - Examples: Address Verification, Credit Card Payment
- Composite Web Service (course grained)
  - Stateful, orchestration of base services
  - Implement complex business processes
  - Usually implemented in BPEL (industry standard for web services process flow)
  - Examples: Payment, Professional License, Business Permit
- REST (HTTP-Get)
  - Everything in the URL (no SOAP or WSDL)
  - http://api.local.yahoo.com/LocalSearchService/V1/localSearch?appid=YahooDemo&query=pizza&zip=95661&results=2
    - Returns first two pizza places found in Roseville, CA

SOAP (XML Document)

- Simple Object Access Protocol
- A simple XML based protocol to let applications exchange information over HTTP
- SOAP is a protocol for accessing a Web Service

WSDL (XML Document)

- Web Service Definition Language
  - Interface
    - Web Methods (service actions)
  - Service
    - Name, Description, Namespace
    - Location (service URL)
  - WSDL can be placed in a UDDI repository
    - Public directory of available services
  - Interface Only vs Deployment documents

Standards - General

- Organizations
  - W3C
  - OASIS
- SOAP, XML, WSDL, UDDI
- WSIL (Web Services Inspection Language)
  - May replace UDDI
- WSRP (Web Services for Remote Portlets)
  - Descriptive GUI
- WS-Reliability, WS-ReliableMessaging

Standards - Process

- BPEL (Business Process Execution Language)
  - OASIS - IBM, Microsoft, BEA
- WSCL (Web Services Conversation Language)
  - HP
- WSCI (Web Services Choreography Interface)
  - BEA, Sun, SAP
- BPML (Business Process Markup Language)
  - W3C
- BPSS (Business Process Specifications Schema)
  - ebXML
- WSFL (Web Services Flow Language)
  - IBM
- XLANG

Standards - Transaction

- WS-Transaction
- WS-Coordination
  - Atomic
  - Business Activity (long running)

Reference Enterprise Architecture

- Set architecture direction
- Browser-based applications
- Web services based
- Common components
  - Business rules engine
  - Enterprise services
  - Shared services
  - Directory services
- Three platforms
  - .NET
  - J2EE
  - Mainframe
- Application & Services Integration

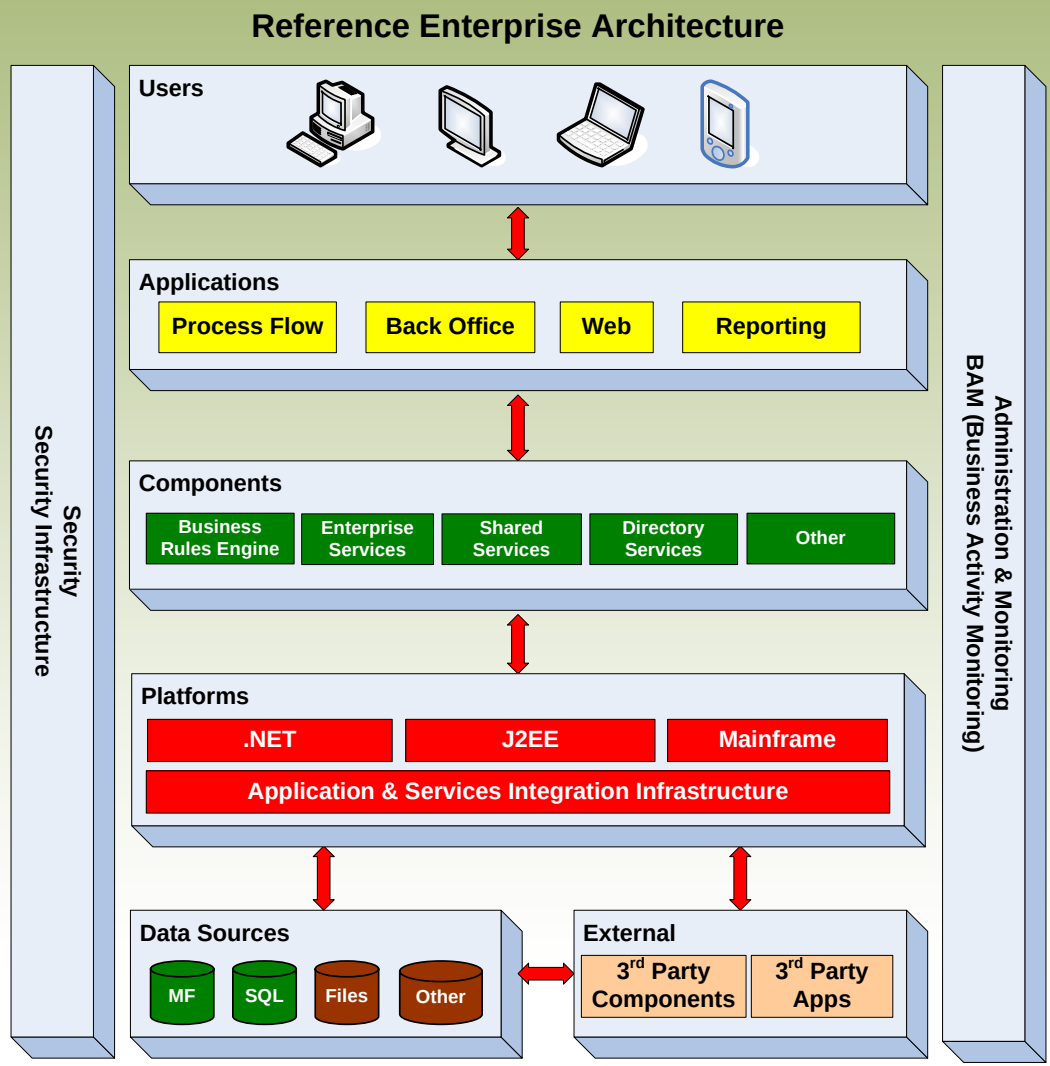
Ref Arch – Enterprise Services

- State-wide scope
- Recommended mandatory usage
- May be COTS/Packaged Application
  - HR, Admin, Financial, Asset Management
  - Enterprise Search
  - RSS (Subscription/Alerts/FAQs/News)

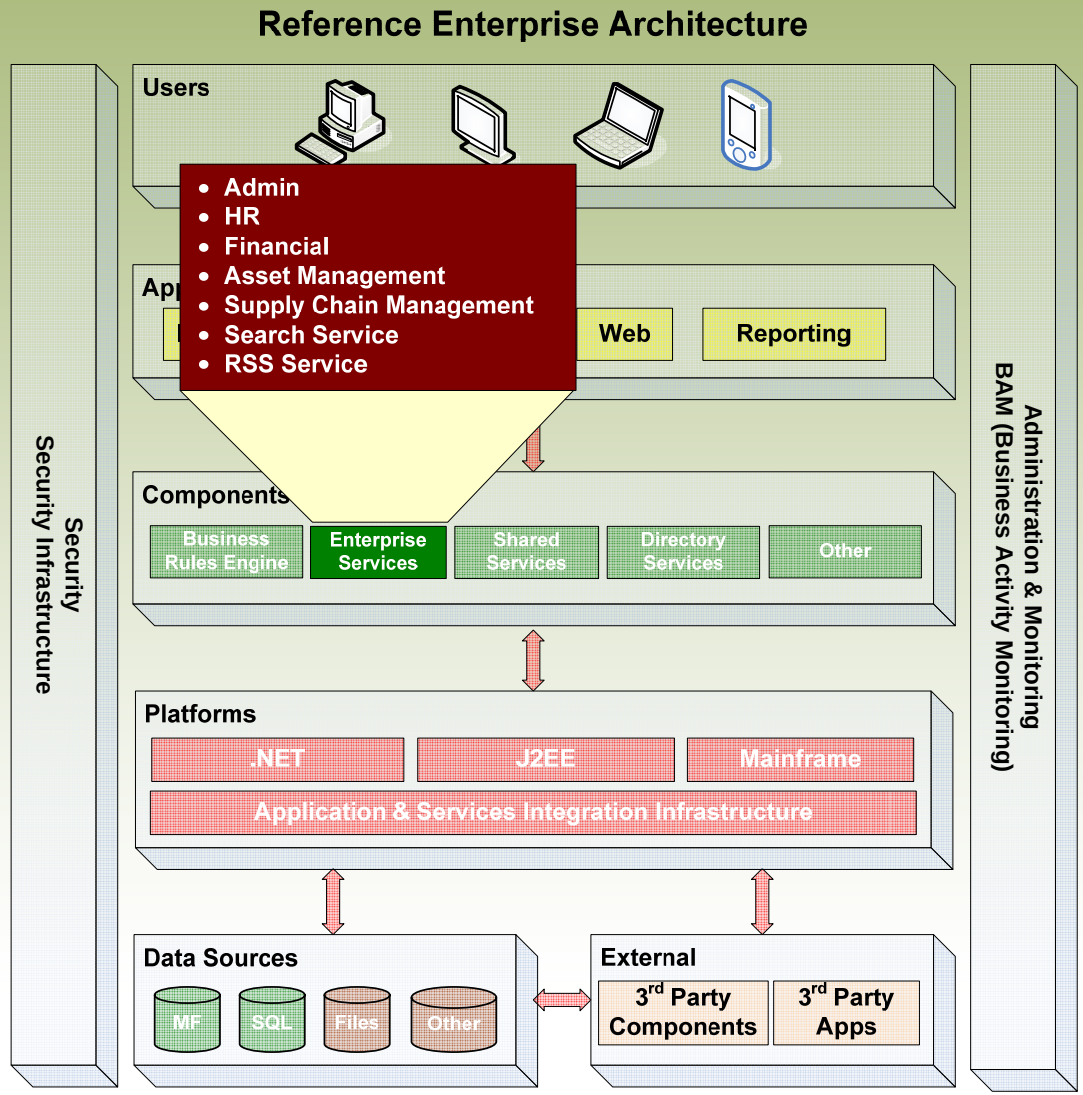
Ref Arch – Shared Services

- Community of Interest scope
- Consumed by applications
- Shared services – single development org
  - Address Verification Service
- Shared services – multiple dev organizations
  - GIS Web Services
- Composite Shared Services
  - Payment Service

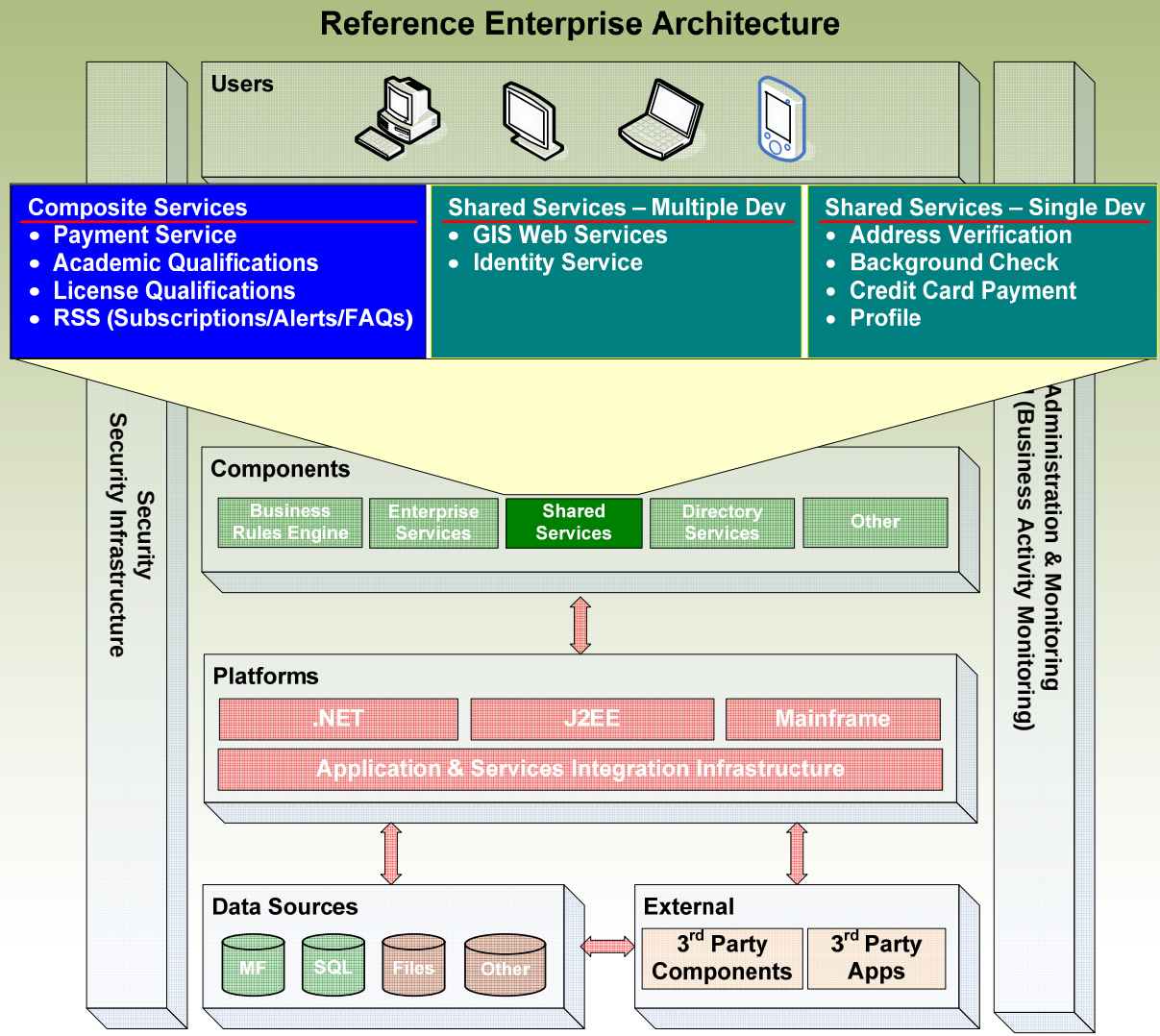
Reference Architecture



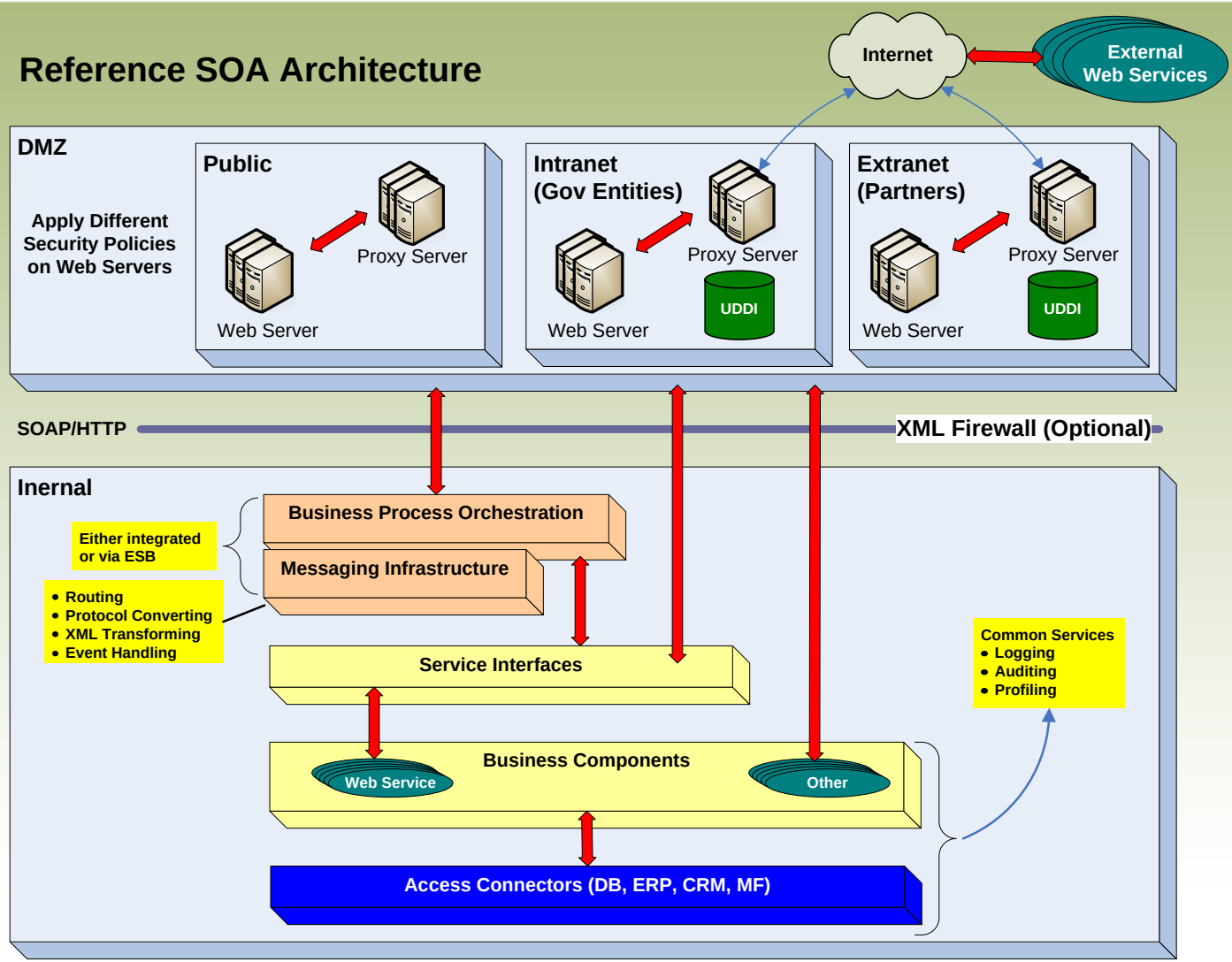
Ref Arch - Enterprise Services



Ref Arch - Shared Services

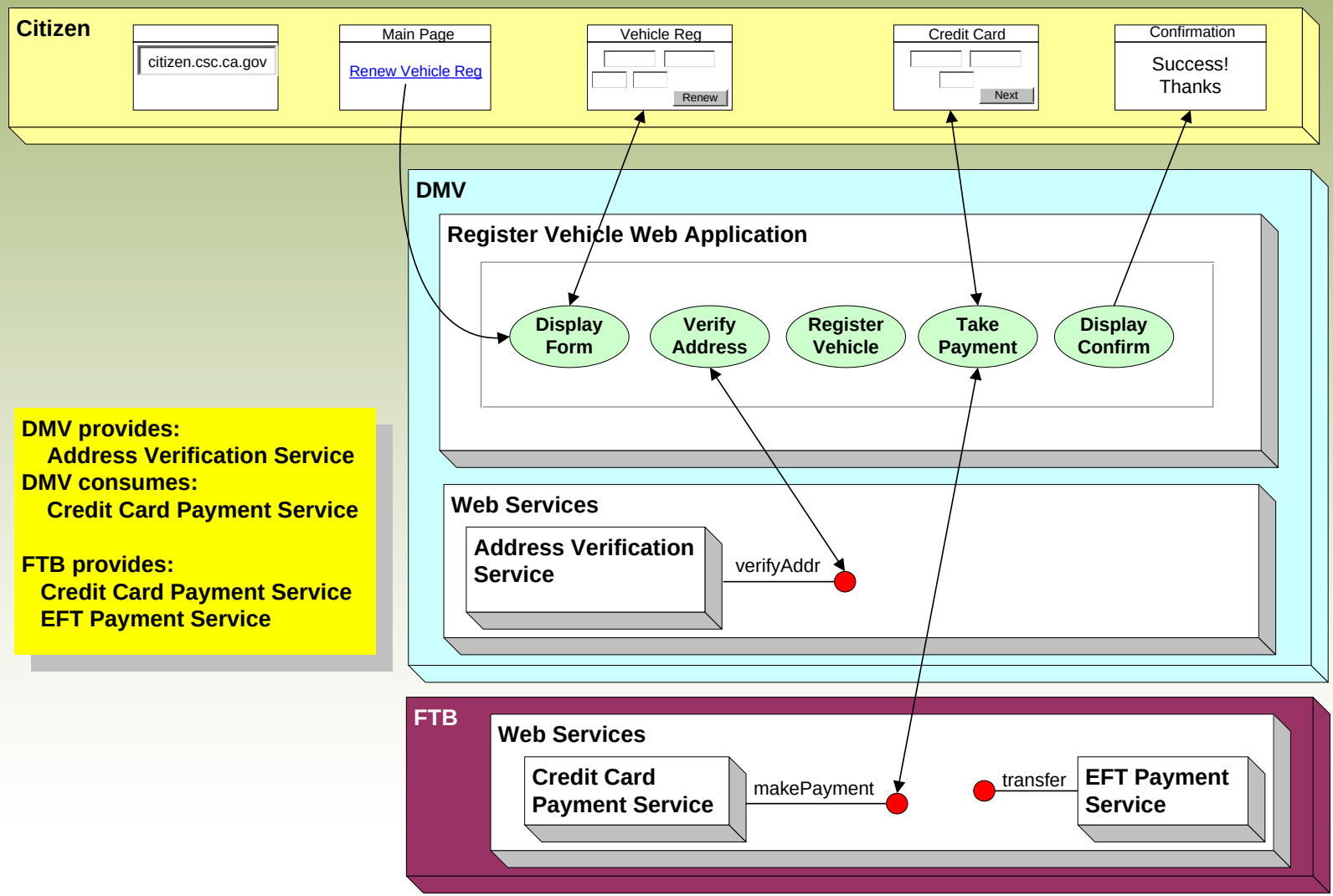


Reference Architecture

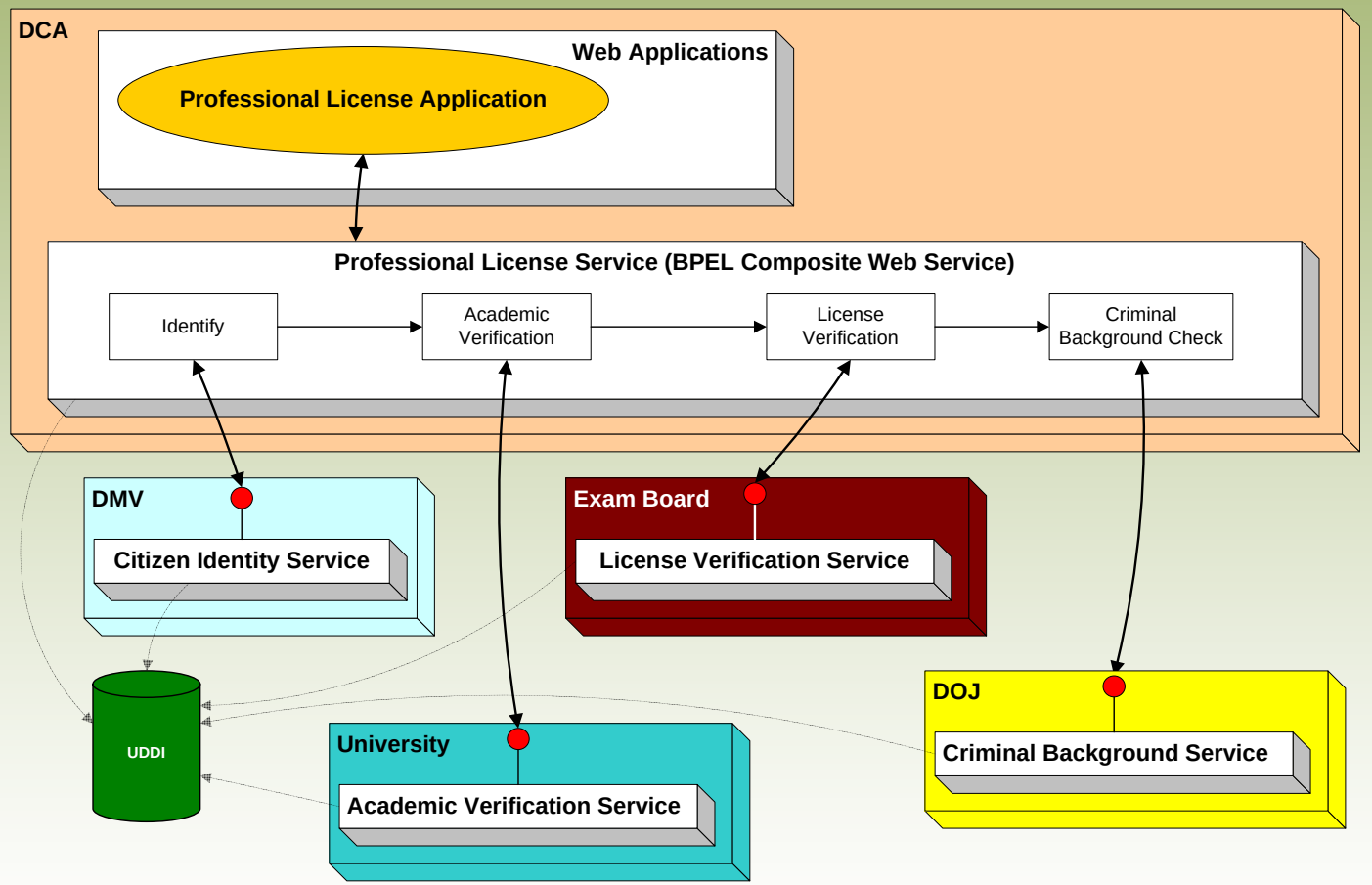


Some Patterns

Web App Consuming WS

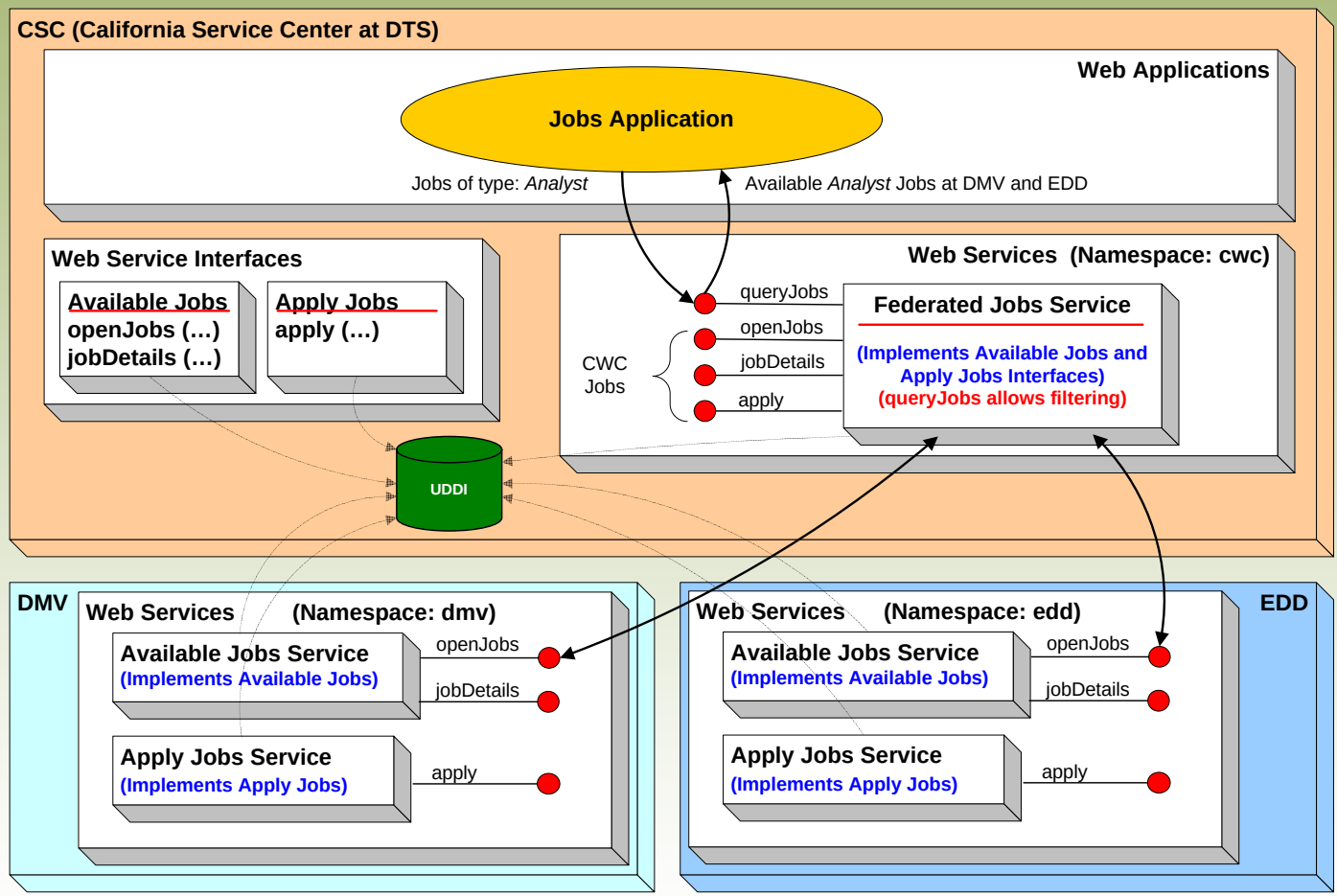


Composite Web Service



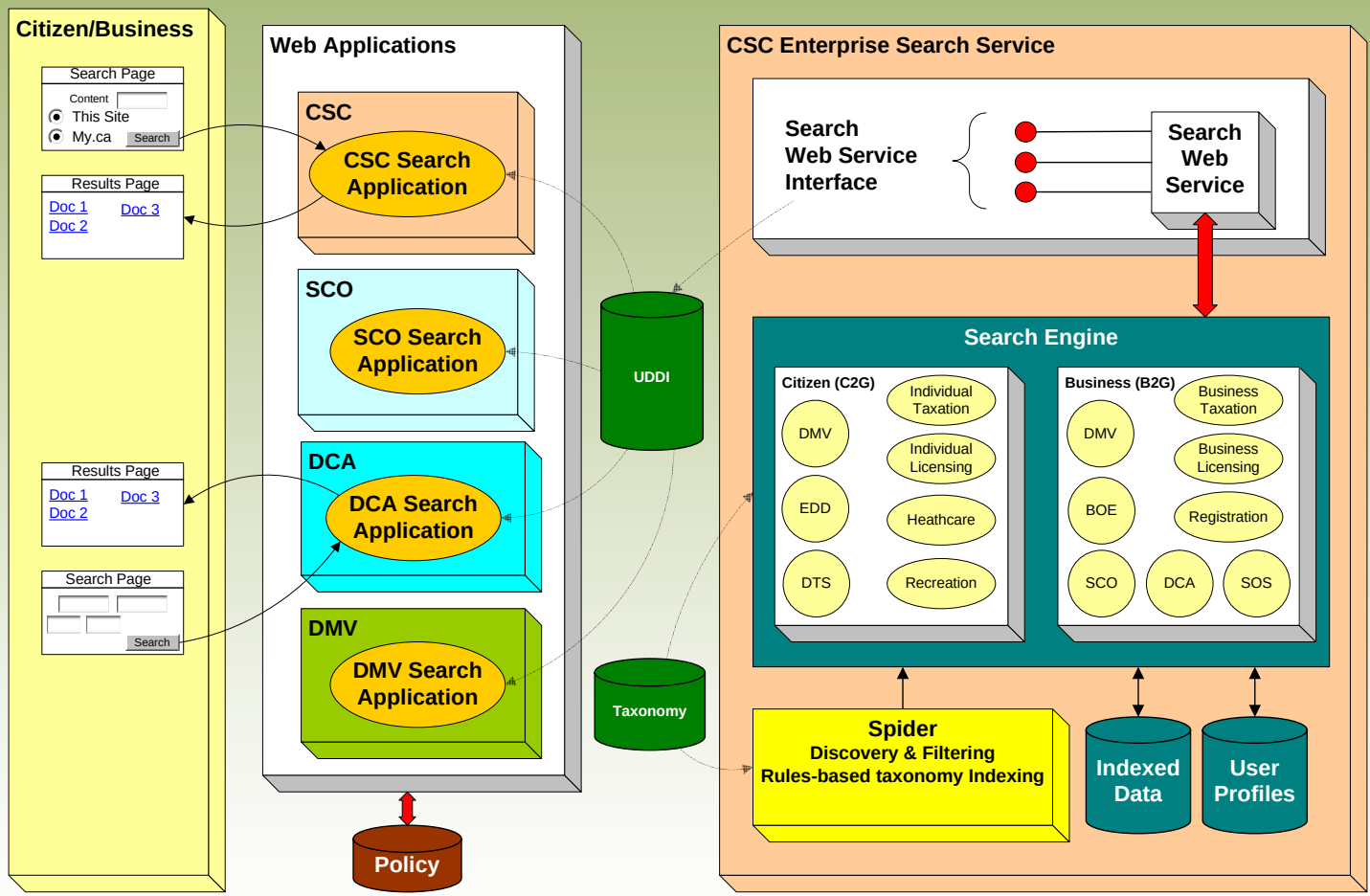
DCA Applicaton calling Composite web service, which calls other web services.

Federated Web Service



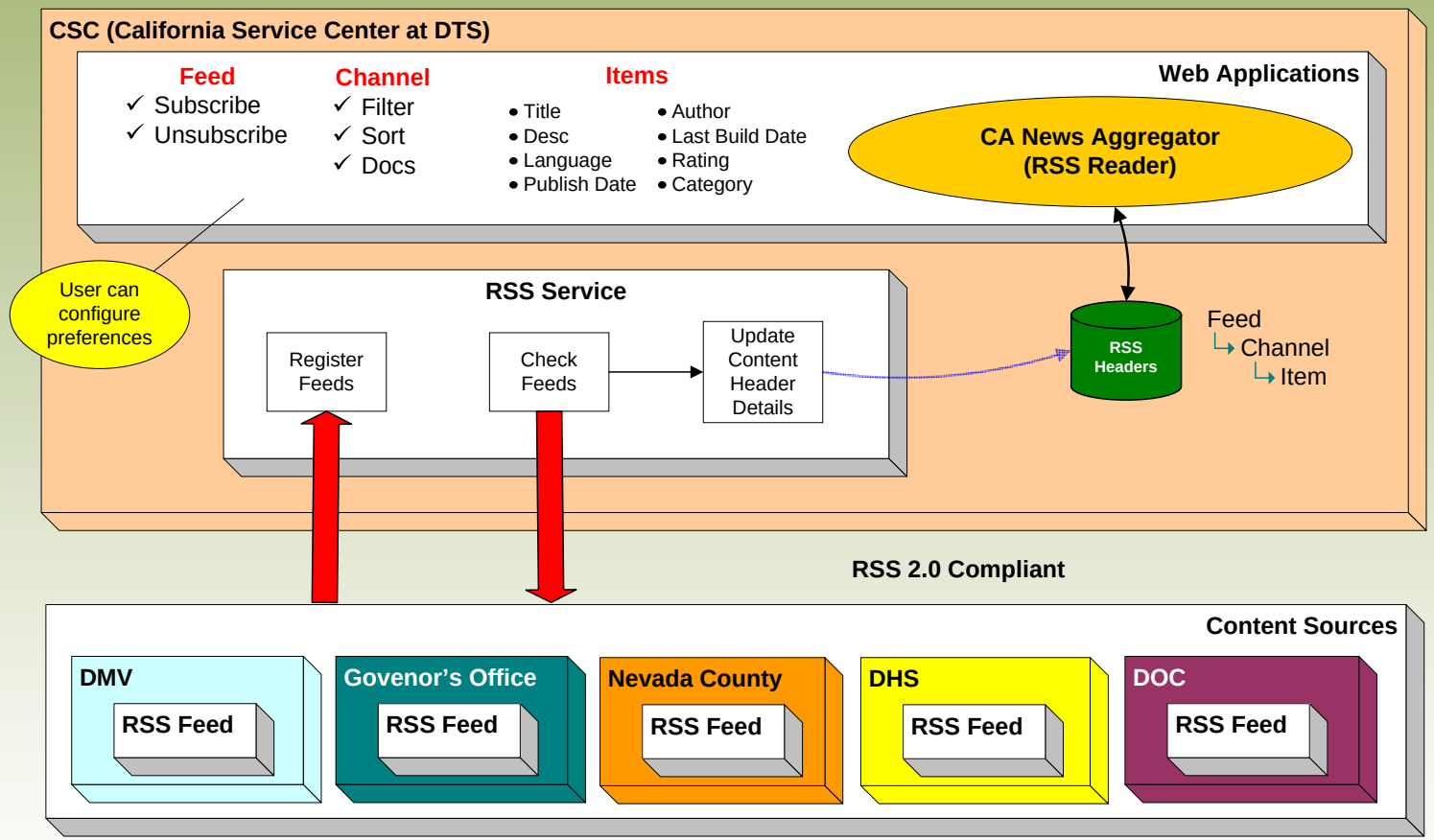
1. CSC Applicaton federated web service.
2. Services implementing the same interfaces.
3. Federated WS calling other web services.

Enterprise Search Service



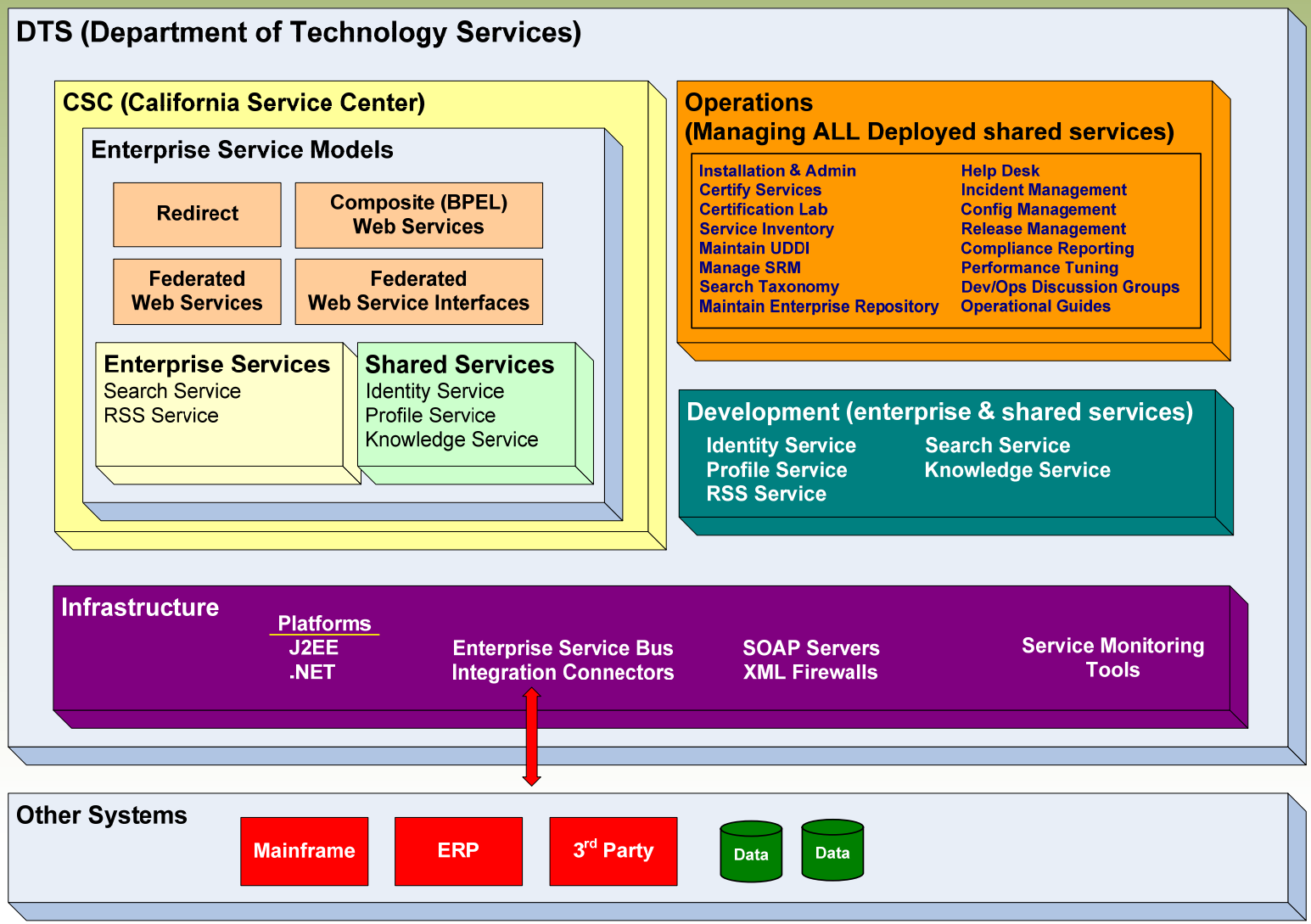
Content remains in departments. Indexes are centralized.

Subscriptions/Alerts/News/FAQs



1. CSC RSS Reader Applicaton dynamically displays feed information based on user's subscription preferences.
2. RSS Service automatically updates feed changes every 5 minutes (configurable).

DTS Example


DTS (Department of Technology Services)
CSC (California Service Center)
Enterprise Service Models
Redirect
Composite (BPEL) Web Services
Federated Web Services
Federated Web Service Interfaces
Enterprise Services
Search Service
RSS Service
Shared Services
Identity Service
Profile Service
Knowledge Service
Operations
(Managing ALL Deployed shared services)
Installation & Admin
Certify Services
Certification Lab
Service Inventory
Maintain UDDI
Manage SRM
Search Taxonomy
Maintain Enterprise Repository
Help Desk
Incident Management
Config Management
Release Management
Compliance Reporting
Performance Tuning
Dev/Ops Discussion Groups
Operational Guides
Development (enterprise & shared services)
Identity Service
Profile Service
RSS Service
Search Service
Knowledge Service
Infrastructure
Platforms
J2EE
.NET
Enterprise Service Bus
Integration Connectors
SOAP Servers
XML Firewalls
Service Monitoring Tools
Other Systems
Mainframe
ERP
3rd Party
Data
Data

Legacy Integration Patterns

Integration Platforms

- Enterprise Service Bus (examples)
  - IBM Websphere ESB

    http://www-306.ibm.com/software/info1/websphere/index.jsp?tab=landings/esb
  - Oracle Fusion

    http://www.oracle.com/products/middleware/index.html
  - Cape Clear

    http://www.capeclear.com/products/cc6.shtml
  - Sonic Software

    http://www.sonicsoftware.com/products/sonic_esb/index.ssp
- Microsoft Biztalk/WCF (Windows Vista)

WS Interface on MF Apps

- SoftwareAG EntireX
  http://www.softwareag.com/Corporate/products/entirex/default.asp
- SoftwareAG ApplinX
  http://www.softwareag.com/Corporate/products/applinx/default.asp

Makes mainframe applications (particularly Natural and Adabas) look like web services. EntireX executes on the mainframe and exposes the service interfaces. ApplinX solution requires no changes to mainframe code.

COBOL as WS Language

Fujitsu Consulting provides a COBOL compiler for a variety of platforms and languages. For example, NetCOBOL for .NET is a COBOL compiler created specifically for Microsoft's .Net Framework. This means that COBOL is just another .NET scripting language (like VB.NET, C#, J#, etc.). This allows COBOL code to be mixed with C# or VB.NET code. It compiles to Microsoft MSIL (language neutral, .NET runtime) code.

- NetCOBOL main page

  http://www.netcobol.com/products/

- NetCOBOL for .NET

  http://www.netcobol.com/products/windows/netcobol.html

Rewrite/Create New Apps

- Retire existing app, rewrite in Java or .Net
- Use SOA (web services-based architecture)
- Opportunity to re-engineer data model
- Opportunity to re-engineer business processes, business rules, business logic

Web Services Security

Standards - Security

- WS-Security
  - Top level web services security management
- WS-Trust
  - Framework for security tokens
- WS-Provisioning
  - Federate identity management
- WS-Federation
  - Broker trust relationships in federated environment
- WS-Addressing
  - Specify Identification and addressing information
- WS-Authorization
  - Manage authorization data and policies
- WS-Policy
- WS-Privacy
- SAML (Security Assertion Markup Language)
- STS (Secure Token Service)

SOA Security

- Organizations
  - W3C, IETF, OASIS
- XML Security for Web Services (W3C)
  - XML Signatures (XMLDS)
    - Defines the processing rules and syntax to wrap message integrity, message authentication, and user authentication data inside an XML format.
  - XML Encryption
    - Encrypted data is wrapped inside XML tags
- WS-Security (OASIS)
  - Defines the mechanism for including integrity, confidentiality, and single message authentication features within a SOAP message
  - Uses XML Signatures and XML Encryption

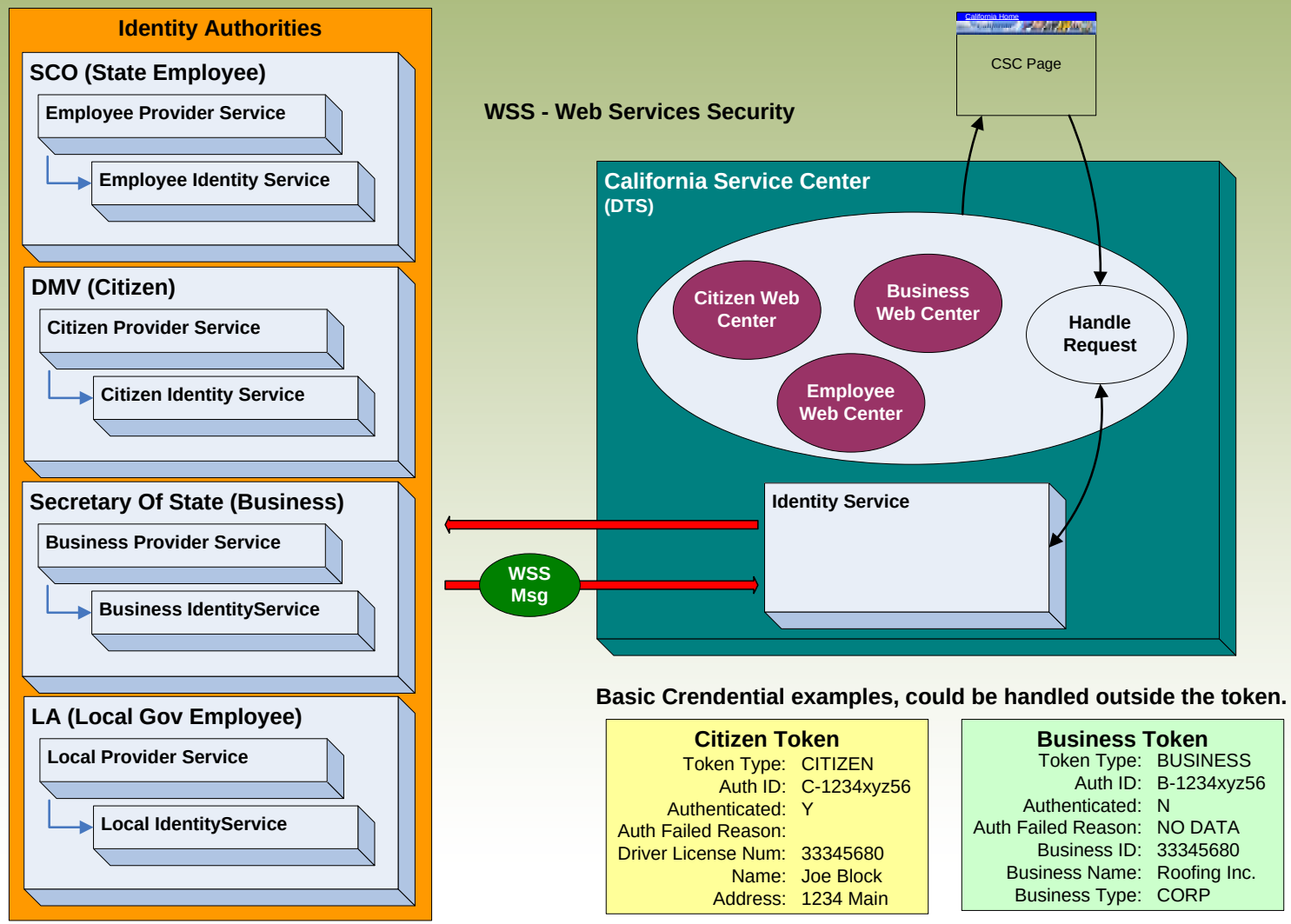
SOA Security

- SAML – Security Assertion Markup Language
  - Standard protocol for sharing security information
- XACML (eXtensible Access Control Markup Language
  - Defines a vocabulary to specify subjects, rights, objects, and conditions
- Digital Signatures
  - Keys used to produce and verify digital signatures

SOA Security

- Certificates
  - A data structure that holds the identification and public key of the certificate owner

Security - Identification



Basic Crendential examples, could be handled outside the token.

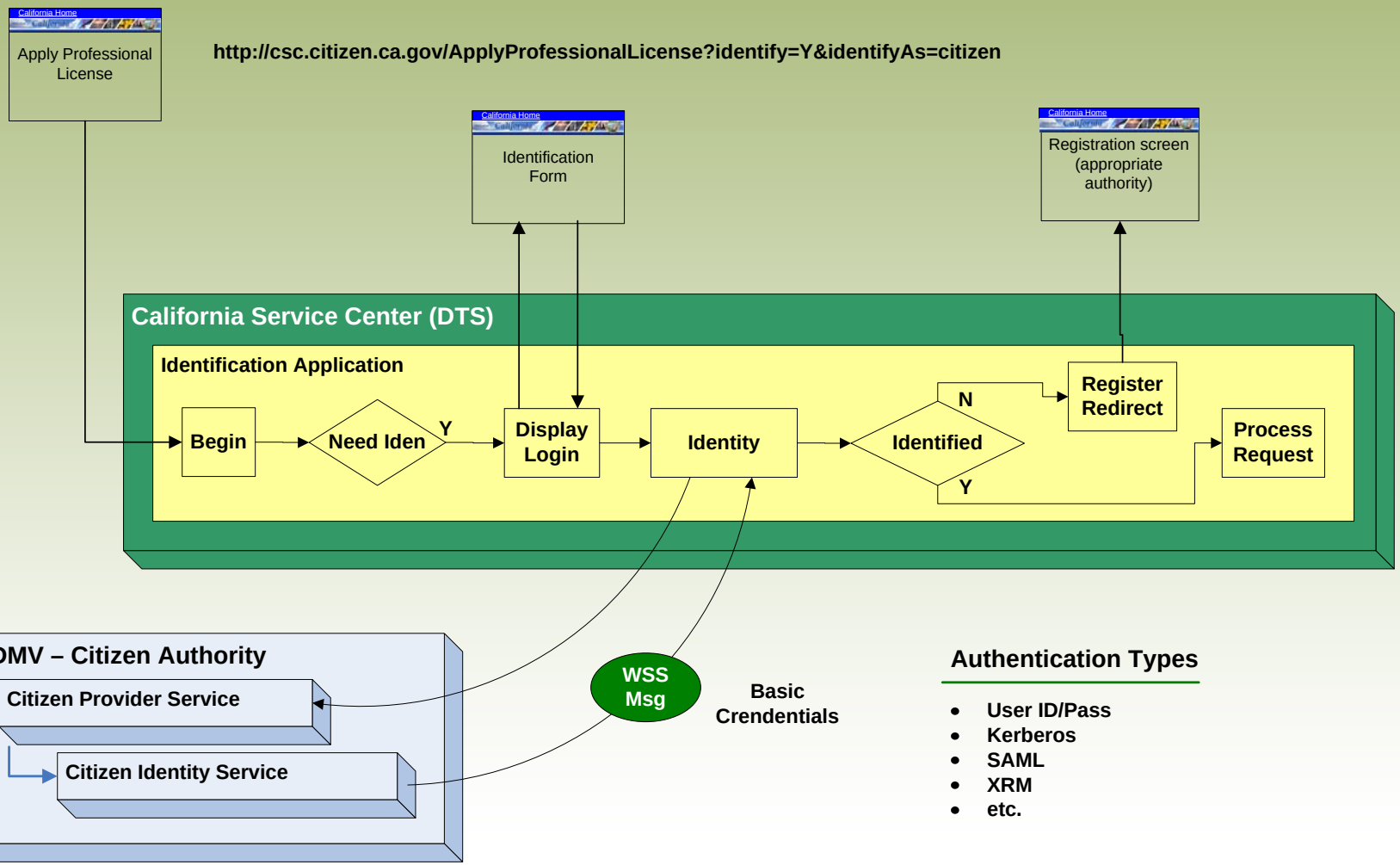
Citizen Token

Token Type:	CITIZEN
Auth ID:	C-1234xyz56
Authenticated:	Y
Auth Failed Reason:	
Driver License Num:	33345680
Name:	Joe Block
Address:	1234 Main

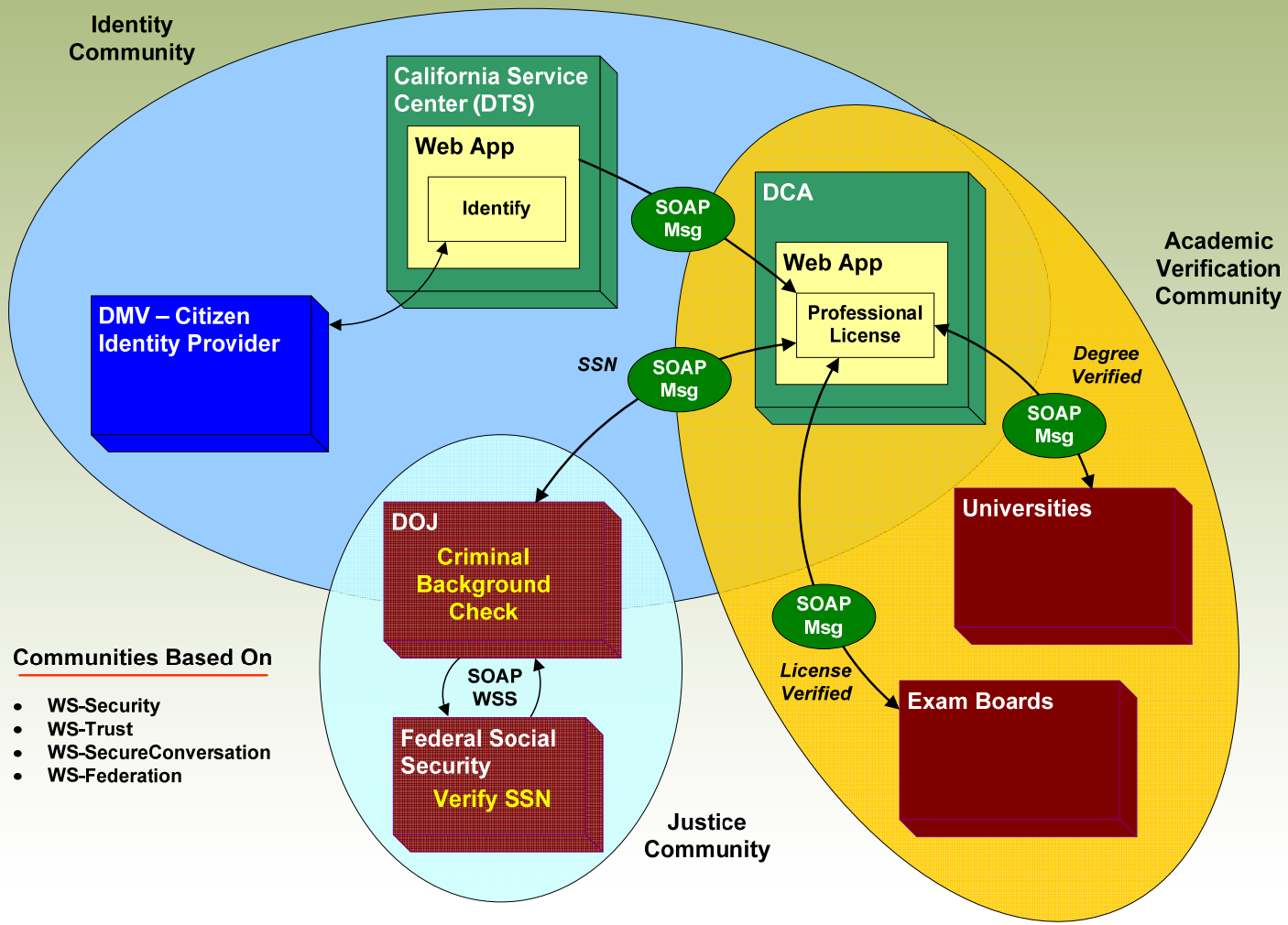
Business Token

Token Type:	BUSINESS
Auth ID:	B-1234xyz56
Authenticated:	N
Auth Failed Reason:	NO DATA
Business ID:	33345680
Business Name:	Roofing Inc.
Business Type:	CORP

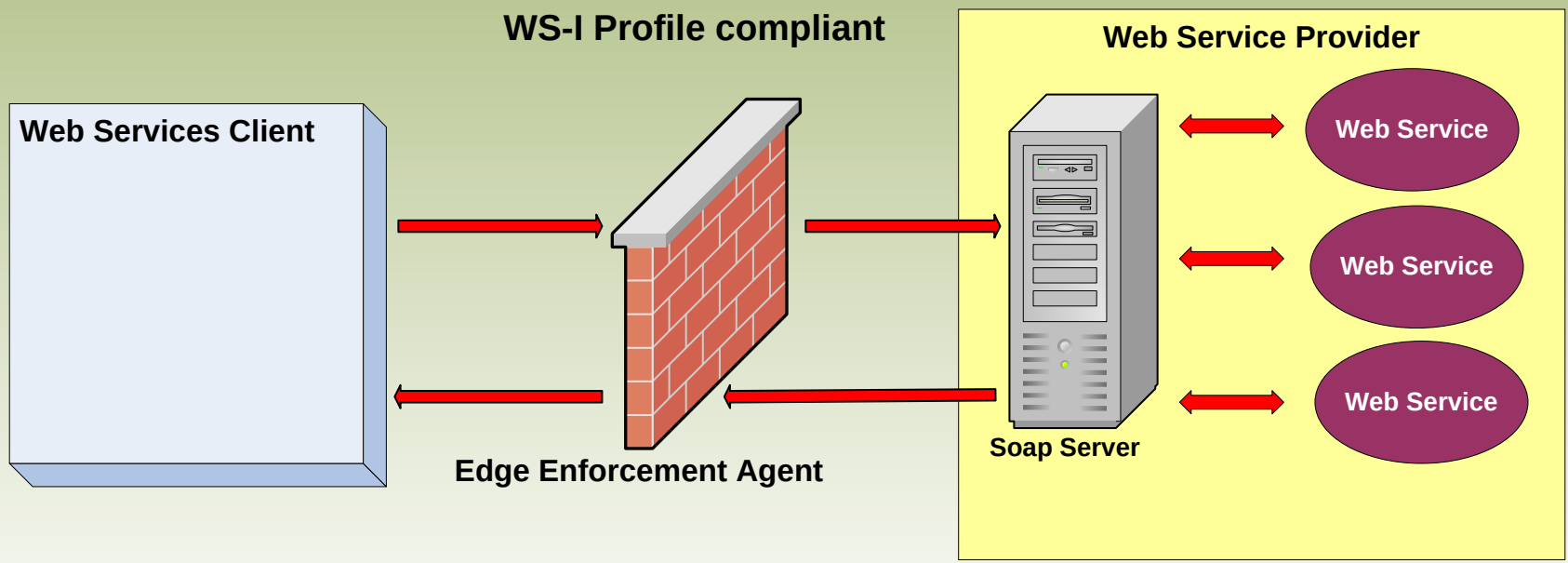
Security – Citizen Service



Security – Circle of Trusts



Security – XML Firewalls



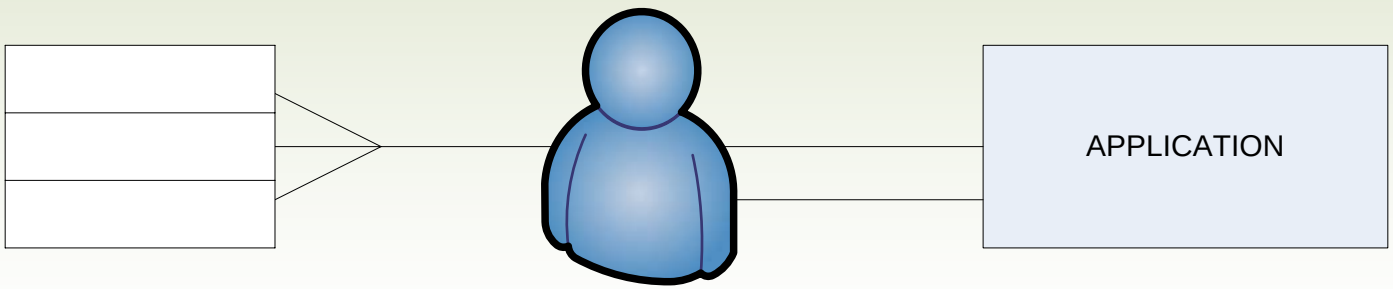
The Edge agent must look inside the SOAP/WSS messages and enforce security access to the SOAP server.

Identity Management and Authentication

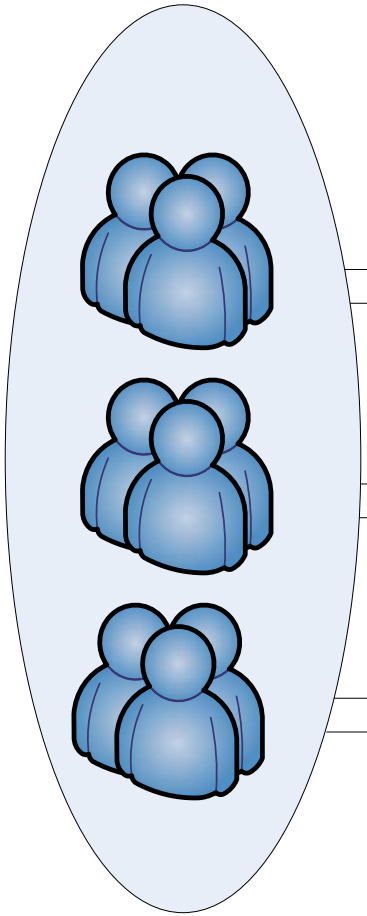
Identity Today

- Identity silos
- Duplicate processes
- Duplication of constituent data
- Inconsistent identity practices

- Interoperability disconnects
- Tight coupling
- No governance in Identity space



Identity Chaos



APPLICATION 1

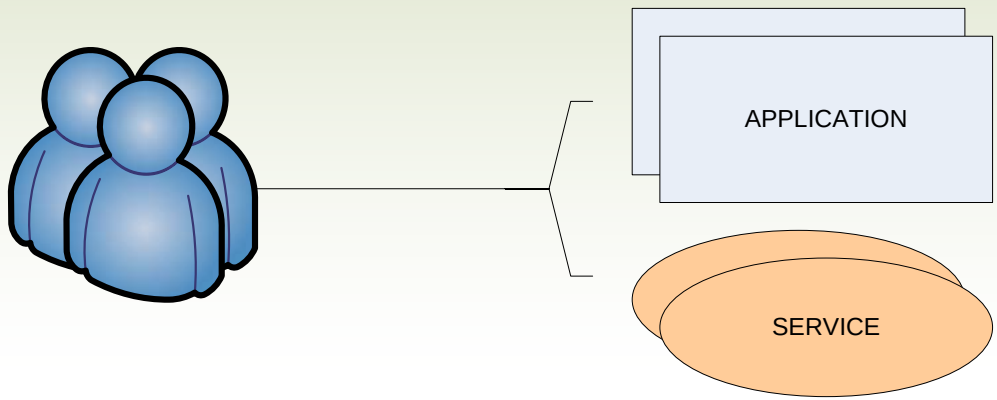
APPLICATION 2

APPLICATION 3

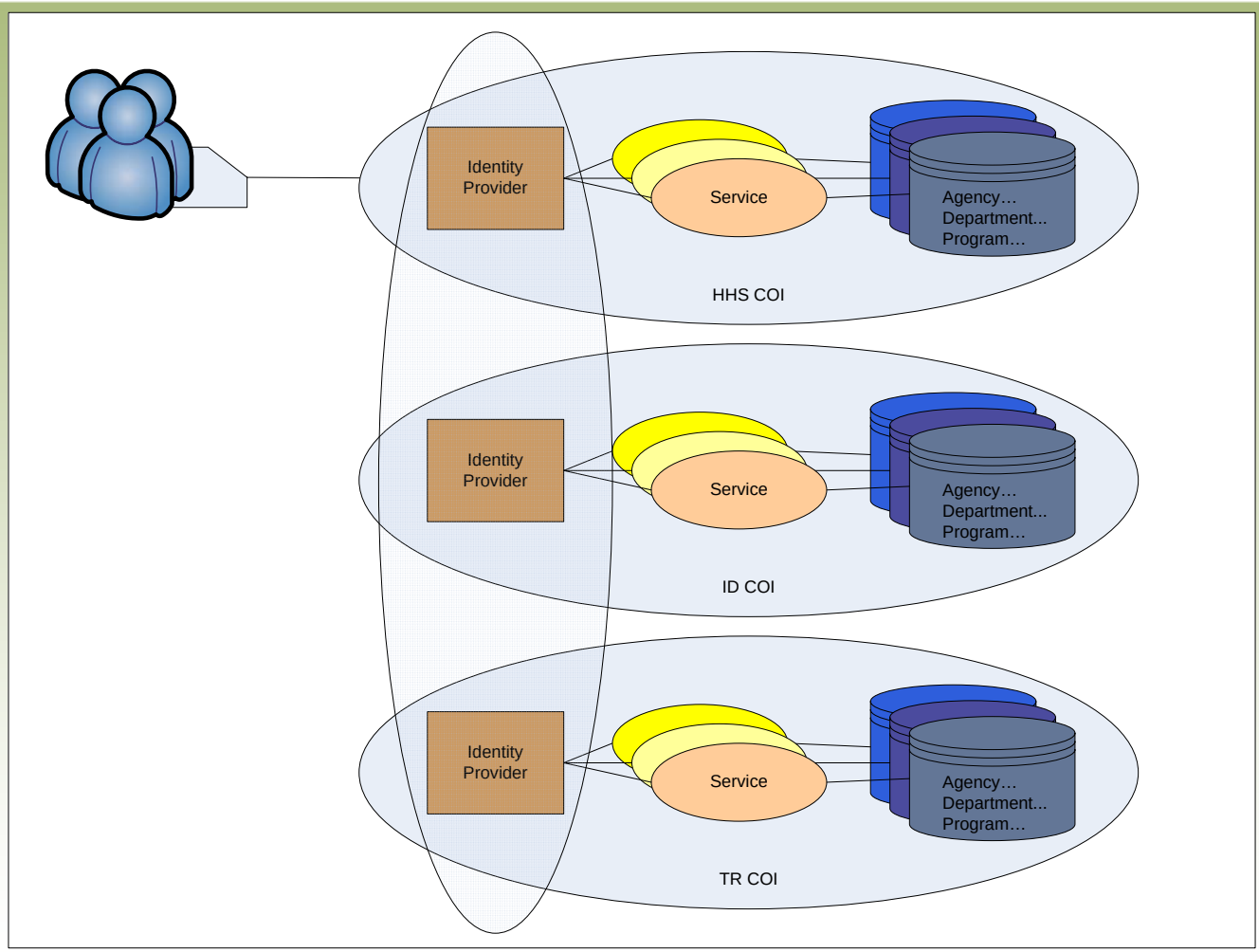
- Single Population
- Duplicated at each system
- Higher management/maintenance costs
- Inefficient design

Identity Tomorrow

- De-coupled from the application
  - Identity component
  - Authentication component
- Service Oriented Approach
- Managing required elements
- Consistent identity practices
- Consistent security



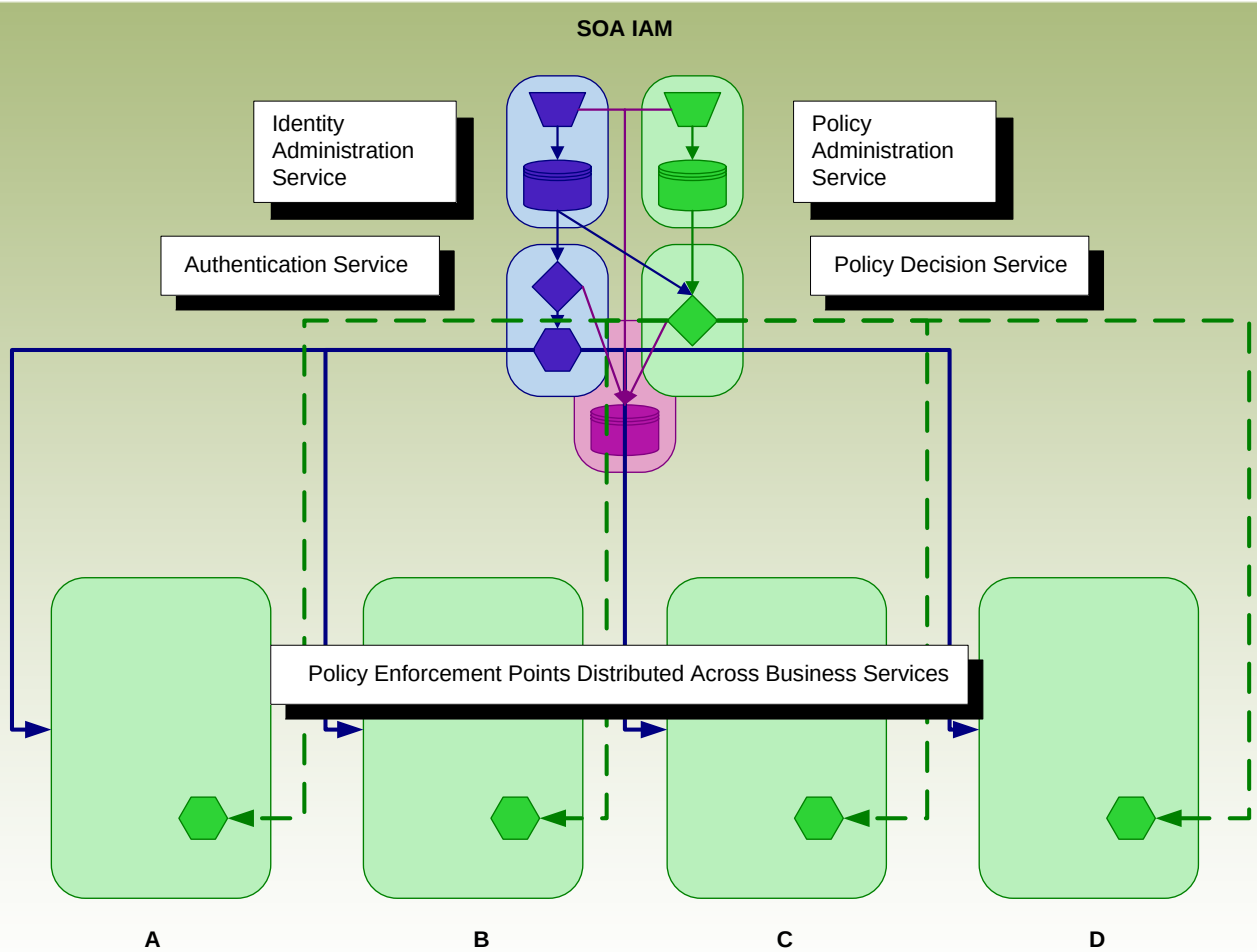
In Federation



Why Now?

- SOA enables federated identity and federation
- Standards maturation provides the ability to communicate in common terms
- Products are increasingly being made more interoperable (standards-based)
- Technology allows us to re-engineer the identity process in the Internet/web space
- Identity is in disarray

Identity and SOA



Source: Gartner – A Functional Model Aids Understanding of Identity and Access Management Tools

The Benefits

- Offloading business processes
- Consistent:
  - Policy across COI
  - Security
  - Identity practices
  - Audit/trace capabilities and practices
  - Accountability
- Administration
  - Fewer identities to directly manage
    - Role-based assignment of resources
- Reusable components
- Governance in Identity space

The Risks

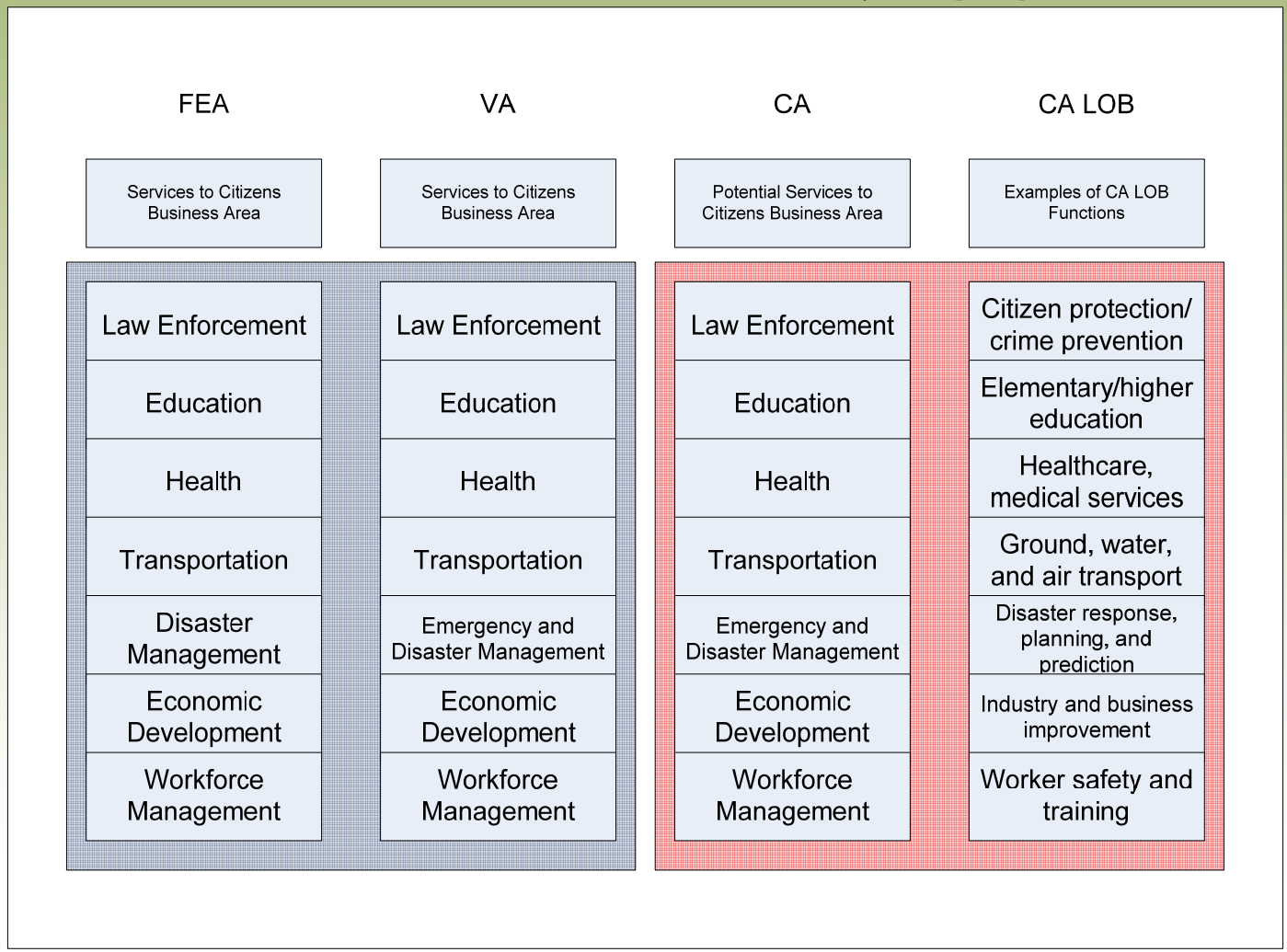
- Security
  - Intrusion, auditing, internal threat, etc.
- Federated identity issues
- Privacy
  - Policy
  - Opt-in
- Lack of mature implementations
- Funding cycle – FSR review & development
- Public perception
- Culture shock
- Governance in identity space

How?

- Stepwise approach
- Assess climate (not technology)
  - What existing partnerships could facilitate?
  - What business obstacles exist?
- Define standards to-be
  - Federation
  - Communities of Interest
    - Based on federation standards
    - Roles
  - Security
  - Interactions
- The right people?

Possible COI delineation

Business Reference Model: Federal and State Comparison [Draft]



CEAP Contacts

- Steve Clemons (Director Enterprise Architecture)
  - Steve.Clemons@ceap.ca.gov 916-454-8198
- Lee Macklin (SOA)
  - Lee.Macklin@ceap.ca.gov 916-739-7637
- Sjon Woodlyn (Identity)
  - Sjon.Woodlyn@ceap.ca.gov 916-657-7581
- SOA Powerpoint / SOA Details

  http://www.cio.ca.gov/ITCouncil/Committees/ArchStandards.html

Questions